

ABSTRACT

Method for processing encoded data for a first domain received in a network pertaining to a second domain

The invention relates to a method of processing data (LECM1), encrypted according to an encryption method specific to a first domain such that they cannot be decrypted without the aid of a first secret (K_{N1}) specific to the first domain, these data being received in a presentation device (202) connected to a network belonging to a second domain. The method comprises the steps consisting, for the presentation device, in:

(a) transmitting (404) to a processing device (211) connected to the network at least a portion ($E\{K_{N1}\}(K_C)$) of said encrypted data;

(b) receiving (408) from said processing device (211) at least one element ($E\{K_{N2}\}(K'_C) || E\{K'_C\}(K_C)$) being used to decrypt said received data with the aid of a second secret (K_{N2}) specific to the second domain, the second secret being contained in the presentation device.

Figure 4.